REMARKS

This supplemental amendment seeks to overcome prior art to Raz (US Patent Application Publication No. 2008/0016566) cited in a previous official action.

Claims 1-8, 10, 11, 13-16, 20, 33, 35 and 46-69 are currently pending in the Application. In the present response, claims 3 and 57 are cancelled without prejudice. Claims 1, 46, 49, 55, 56 and 66 are amended.

Applicants express their appreciation to Examiner Frantz Jean for the courtesy of a personal interview, which was granted to Applicants' representative, Sanford T. Colb (Reg. No. 26,856), on January 27, 2009, at the USPTO. The substance of the interview is set forth in the Interview Summary.

In the interview, claims 1-8, 10, 11, 13-16, 20, 33, 35 and 46-69 were discussed vis-à-vis the prior art to Raz. The Interview Summary Record states, in relevant part, "Examiner stated that the claims as written are too broad, therefore, are not defined over Raz. Suggestions were made to applicant's representative, Attorney Colb, to incorporate dependent claims 3 and some other dependent claims to the independent claims. Mr. Colb will consult with client for approval".

As agreed with the Examiner, Applicant has amended independent claims 1, 46, 49, 55 and 66 to include the subject matter of claims 3 and 43. Applicant has also amended independent claim 56 to include the subject matter of claim 57. The independent claims now recite, inter alia, the filtering including detecting at least one of a traffic pattern which differs from an expected traffic pattern and a traffic volume which differs from the expected volume, which expected pattern and or volume are determined during a period in which the victim is not at an overload condition, by determining whether the traffic pattern and/or volume vary statistically significantly from any of the expected pattern and volume, respectively.

Raz describes: "coordinated SYN denial of service (CSDoS) attacks are reduced or eliminated by a process that instructs a layer 4-7 switch to divert a small fraction of SYN packets destined to a server S to a web guard processor. The web guard processor acts as a termination point in the connection with the one or more clients from which the packets originated, and upon the establishment of a first TCP connection with a legitimate client, opens a new TCP connection to the server and transfers the data

between these two connections. It also monitors the number of timed-out connections to each client. When a CSDoS attack is in progress, the number of the forged attack packets and hence the number of timed-out connections increases significantly. If this number exceeds a predetermined threshold amount, the web guard processor declares that this server is under attack. It then reprograms the switch to divert all traffic (i.e. SYN packets) destined to this server to the web guard processor" (Abstract).

However, as discussed with the Examiner during the interview, Raz does not show or suggest detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, the expected pattern and the expected volume being determined during a period in which the victim is not at an overload condition, and wherein the detecting step includes determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

Accordingly, independent claims 1, 46, 49, 55 and 66 have been amended to incorporate the limitations of claims 3 and 43, which include, inter alia, detecting any of (i) a traffic pattern that differs from an expected pattern and (ii) traffic volume that differs from an expected volume, the expected pattern and the expected volume being determined during a period in which the victim is not at an overload condition, by determining whether any of the traffic pattern and volume varies statistically significantly from any of the expected pattern and volume, respectively.

Additionally, independent claim 56 has been amended to recite the limitation of claim 57, including, inter alia, performing a statistical analysis by learning an expected traffic pattern of the flows while the victim is not under attack and is not in an overload condition, and detecting an attack by determining that the anomalous pattern differs statistically significantly from the expected traffic pattern.

Thus, Raz does not show or suggest the present invention as recited in independent claims 1, 46, 49, 55, 56 and 66.

With reference to the above discussion, independent claims 1, 46, 49, 55, 56 and 66 are deemed patentable over the prior art to Raz and favorable reconsideration is respectfully requested. Claims 2, 4-8, 10, 11, 13-16, 20, 33, 35, 47-48, 50-54, 58-65 and 67-69 each depend directly or ultimately from one of the above mentioned independent claims and recite additional patentable subject matter and therefore are deemed

patentable.

In view of the foregoing remarks and amendments, all of the claims are deemed to be allowable. Favorable consideration and allowance of the application is respectfully requested.

No fee is believed due. However, the Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 141449, under Order No. 103376-3.

Respectfully submitted,

/Joshua T. Matt/
Joshua T. Matt (Reg. No. 55,435)
Attorney for Applicants
Nutter McClennen & Fish LLP
World Trade Center West
155 Seaport Boulevard
Boston, MA 02210-2604

Tel: (617) 439-2000
Fax: (617) 310-9000

Date: March 25, 2009

1816825.1